جلسه چهارم:

امنیت کامل: $\forall m, c \quad Pr[C=c] > 0$

$Pr[M=m | C=c] = Pr[M=m]$

↳ OTP رمز یکبار مصرف

ضعیف‌تر کردن تعریف امنیت:

1. concrete approach:

مهاجم به زمان + محدود می‌شود

احتمال موفقیت مهاجم در آزمایش امنیت به ε محدود می‌شود.

سیستم رمز Π ، (t, ε)-امن است.

یادآوری: آزمایش امنیت $PrivK^{eav}_{\Pi, A}$:

1. $k \leftarrow Gen$
2. $m_0, m_1 \leftarrow A$
3. $b \in \{0,1\}$
4. $c \leftarrow Enc_k(m_b)$
5. $b' \leftarrow A(c)$

$PrivK^{eav}_{\Pi, A} = 1 \iff b = b'$

سیستم امنیت کامل دارد اگر

$Pr[PrivK^{eav}_{\Pi, A} = 1] = \frac{1}{2}$

۲. Asymptotic approach:

مهاجم محدود می‌شود به زمان چند جمله‌ای

مهاجم می‌تواند احتمالاتی باشد

احتمال موفقیت مهاجم در آزمایش امنیت ناچیز باشد.

← پارامتر امنیتی : n

سیستم Π با پارامتر امنیتی n، امن است اگر برای هر مهاجم احتمالاتی چند جمله‌ای (PPT)، احتمال موفقیت مهاجم در آزمایش امنیت حداکثر $negl(n)$ باشد. (ناچیز باشد).

- امنیت معنایی : semantic security

امنیت تمایزناپذیری ($PrivK^{eav}_{A,\Pi}$)

قضیه: $\Pi = (Gen, Enc, Dec)$ سیستم رمز باشد که امنیت تمایزناپذیری دارد.
برای هر مهاجم PPT A و هر $i \in \{0,1\}^*$، یک تابع ناچیز $negl$ وجود دارد به طوری که:

$$Pr[A(1^n, Enc_k(m)) = m^i] \leq \frac{1}{2} + negl(n)$$

$m \in \{0,1\}^l$

اثبات: فکر شود ت

قضیه: اگر Π سیستم رمز با امنیت تمایزناپذیری باشد، آنگاه برای هر مهاجم PPT A، الگوریتمی مثل A' وجود دارد به طوری که برای هر $S \subseteq \{0,1\}^l$ و هر تابع $f: \{0,1\}^l \to \{0,1\}^l$، یک تابع ناچیز $negl$ وجود دارد به طوری که:

$$\left| Pr[A(1^n, Enc_k(m)) = f(m)] - Pr[A'(1^n) = f(m)] \right| \leq negl(n)$$

$m \in S$

- تعریف امنیت معنایی semantic security :

$\Pi=(Gen,Enc,Dec)$ دارای امنیت معنایی در مقابل مهاجم شنود گر (eavesdropper) است اگر برای هر مهاجم A (PPT) ، الگوریتم A' PPT وجود دارد به طوری که برای هر الگوریتم PPT مانند Samp و هر تابع f و h (با زبان اجرای چند جمله ای) ، تابع ناچیز negl وجود داشته باشد که :

$$\left|Pr\left[A(1^n, Enc_k(m), h(m)) = f(m)\right] - Pr\left[A'(1^n, |m|, h(m)) = f(m)\right]\right| \leq negl(n)$$

که $m \leftarrow Samp(1^n)$.

* قضیه : Π امنیت تمایز ناپذیری داشته باشد $\Rightarrow$ امنیت معنایی نیز دارد. (در مقابل مهاجم شنود گر)

ـ مولدهای شبه تصادفی Pseudorandom Generator (PRG)

یادآوری : OTP :

$Gen : k \leftarrow \{0,1\}^n$

$Enc_k(m) : c = m \oplus k \quad m \in \{0,1\}^n$

$Dec_k(c) : m = k \oplus c$

$|K| = |M| \Rightarrow$ طول کلید بزرگ

نقطه ای از کلید سخت

تعریف PRG : G یک تابع چند جمله ای قطعی باشد که برای هر ورودی $s \in \{0,1\}^n$ ، $G(s)$ رشته ای به طول $l(n)$ (l یک چند جمله ای است) .

G یک مولد شبه تصادفی است ، اگر ویژگی های زیر را دارا باشد :

۱) $\forall n : \quad l(n) > n$

۲) برای هر الگوریتم PPT D ، تابع ناچیز negl وجود داشته باشد به طوری که

$$|Pr[D(G(s))=1] - Pr[D(r)=1]| < negl$$

که $s \xleftarrow{\$} \{0,1\}^n$ ، $r \xleftarrow{\$} \{0,1\}^{l(n)}$